09/831 745

R E P U B L I Q U E  F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

PCT/FR 99 / 02678

REC'D 22 NOV 1999
WIPO PCT

# BREVET D'INVENTION

4

FR99/2678

## CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

**DOCUMENT DE PRIORITÉ**

PRÉSENTÉ OU TRANSMIS CONFORMÉMENT À LA RÈGLE 17.1.a) OU b)

## COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 10 NOV. 1999

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

M Hauet

Martine PLANCHE

SIEGE
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
26 bis, rue de Saint Petersbourg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30



ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

# BREVET D'INVENTION

26bis, rue de Saint-Pétersbourg
75800 Paris Cedex 08
Téléphone: 01 53.04.53.04 Télécopie: 01.42.94.86.54

Code de la propriété intellectuelle-livreVI

REQUÊTE EN DÉLIVRANCE

| | | |
|---|---|---|
| 0 | **RESERVE A L'INPI** | 98 14517 |
| 0-1 | **Date de remise des pièces** | 13/11/1998 |
| 0-2 | **N° d'enregistrement national** | |
| 0-3 | **Département de dépôt** | 99 |
| 0-4 | **Date de dépôt** | 13 NOV. 1998 |
| 0-6 | **Titre de l'invention** | PROCEDE ET DISPOSITIF DE CONTROLE DU CYCLE DE VIE D'UN OBJET PORTATIF, NOTAMMENT D'UNE CARTE A PUCE |
| 0-8 | **Etablissement du rapport de Recherche** | immédiat |
| 0-9 | **Votre référence dossier** | GEM 555 |
| 1 | **DEMANDEUR(s)** | |
| 1-1 | *Nom* | GEMPLUS |
| | *Dénomination sociale* | BRUN Philippe |
| | *Nom de jeune fille* | |
| | *Adresse rue* | Avenue du Pic de Bertagne<br>Parc d'Activités de Gémenos |
| | *Adresse code postal et ville* | 13881, GEMENOS |
| | *Pays* | France |
| | *Nationalité* | France |
| | *Forme juridique* | Autre |
| | *N° SIREN* | 349 711 200 |
| | *Code APE-NAF* | 321B |
| | *N° de téléphone* | 04 42 36 61 32 |
| | *N° de télécopie* | 04 42 36 63 43 |
| | *Courrier électronique* | philippe.brun@gemplus.com |

| | | |
|---|---|---|
| 3 | **INVENTEUR(s)** | |
| 3-1 | *Nom* | GIRAUD |
| | *Prénoms* | Jean Luc |
| | *Adresse rue* | 22 ru du Four |
| | *Adresse code postal et ville* | 13400, AUBAGNE |
| | *Pays* | France |
| | *Société d'appartenance* | GEMPLUS |
| 3-2 | *Nom* | BIRKNER |
| | *Prénoms* | Marc |
| | *Adresse rue* | 2 Résidence St Joseph |
| | *Adresse code postal et ville* | 13950, CADOLIVE |
| | *Pays* | France |
| | *Société d'appartenance* | GEMPLUS |
| 3-3 | *Nom* | TALVARD |
| | *Prénoms* | Laurent |
| | *Adresse rue* | 148 Rue Edmond Rostand |
| | *Adresse code postal et ville* | 13008, MARSEILLE |
| | *Pays* | France |
| | *Société d'appartenance* | GEMPLUS |

| | | | | |
|---|---|---|---|---|
| 4 | **Déclaration de PRIORITE ou REQUETE du bénéfice de la date de dépôt d'une demande antérieure** | Etat | Date | N° de la demande |
| 6 | **Documents et Fichiers joints** | Fichier électronique | Pages | Détails |
| 6-1 | *Description* | gem555.doc | 22 | |
| 6-2 | *Revendications* | gem555.doc | 8 | 29 |
| 6-3 | *Dessins* | gem555.doc | 5 | 12 fig., 1 ex. |
| 6-4 | *Abrégé* | gem555.doc | 1 | --- |
| 6-5 | *Figure d'abrégé* | | | <n°> ex. |
| 7 | **Mode de paiement** | Prélèvement sur compte client | | |
| 7-1 | *Numéro du compte client* | 2381 | | |
| 7-2 | *Remboursement à effectuer sur le compte n°* | 2381 | | |

| | | | | |
|---|---|---|---|---|
| 8 | **REDEVANCES** | Devise | Taux | Montant à payer |
| | *Dépôt* | FRF | 250.00 | 250.00 |
| | *Rapport de recherche (R.R.)* | FRF | 4 500.00 | 4 500.00 |
| | *Déclaration d'un droit de priorité* | FRF | 115.00 | 0.00 |
| | *Revendication à partir de la 11ème* | FRF | 115.00 | 2 185.00 |
| | *Total à acquitter* | FRF | | 6 935.00 |

| | | |
|---|---|---|
| 10 | **Signature** | |
| 10-1 | *Signé par* | Directeur de la Propriété Industrielle<br>NONNENMACHER Bernard<br>GEMPLUS |

La loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

## DOCUMENT COMPORTANT DES MODIFICATIONS

| PAGE(S) DE LA DESCRIPTION OU DES REVENDICATIONS OU PLANCHE(S) DE DESSIN | | | R.M.* | DATE DE LA CORRESPONDANCE | TAMPON DATEUR DU CORRECTEUR |
|---|---|---|---|---|---|
| Modifiée(s) | Supprimée(s) | Ajoutée(s) | | | |
| 23 à 30 | | | RM | 26 mai 1999 | 02 JUIN 1999 - AIR |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Un changement apporté à la rédaction des revendications d'origine, sauf si celui-ci découle des dispositions de l'article R.612-36 du code de la Propriété Intellectuelle, est signalé par la mention «R.M.» (revendications modifées).

# PROCEDE ET DISPOSITIF DE CONTROLE DU CYCLE DE VIE D'UN OBJET PORTATIF, NOTAMMENT D'UNE CARTE A PUCE

L'invention concerne les objets électroniques portatifs tels que les cartes à microcircuits électroniques, dites cartes à puce qui, connectées à des dispositifs électroniques pour permettre à ces derniers de réaliser des fonctions particulières dans le cadre d'une ou plusieurs applications, nécessitent un contrôle de leurs étapes de vie. Lesdites cartes sont en effet généralement utilisées dans des applications (banque, communication, identité, santé...) nécessitant une grande sécurité contre les usages frauduleux. L'invention s'applique plus généralement à tout système embarqué indépendant, doté d'une unité de traitement et des mémoires de programme et de données.

Il est connu dans le monde de la carte à puce que celle-ci résulte d'un assemblage d'un composant (comprenant en général un microprocesseur en relation avec des mémoires via des bus de communication), d'un module (réalisé à l'aide d'un métal conducteur) auquel est relié ledit composant (dans le cadre d'une carte à puce dite à contact) pour permettre audit composant d'être connecté à un dispositif électronique de lecture et/ou écriture (ou coupleur) et d'un corps de carte ou plus généralement d'un support sur lequel est intégré l'ensemble module/composant. Dans la cadre d'une carte à puce dite sans contact, ledit module est remplacé par une antenne et l'ensemble formé par le composant et ladite antenne est intégré au sein dudit support.

La vie d'une carte à puce se décompose généralement en deux ensembles d'étapes se succédant les unes aux autres, correspondant respectivement à la fabrication et à l'exploitation de ladite carte. La composition des deux ensembles d'étapes forme un cycle de vie de ladite carte.

La fabrication d'une carte à puce (à contact ou sans contact) est constituée de plusieurs étapes.

En effet, il est tout d'abord nécessaire de disposer d'un composant électronique qui est initialisé, isolé, puis relié à un module. Ledit composant et le module, auquel il est relié, sont par la suite intégrés sur ou au sein d'un support (généralement un corps de carte plastique) lui même imprimé à des fins d'identification ou de publicité. Par la suite la carte à puce ainsi obtenue est initialisée ou programmée pour répondre aux conditions d'utilisation dans le cadre d'applications.

Le second ensemble d'étapes de vie d'une carte à puce correspond à son exploitation. Cet ensemble peut lui-même être divisé en plusieurs étapes, chacune correspondant, par exemple, à l'implantation ou la suppression de services offerts par la carte à puce à l'utilisateur en fonction de son profil par exemple.

En outre différents acteurs (fabricant de composant, fabricant de cartes à puce, centre de personnalisation de cartes, émetteur de cartes, ou encore porteur de cartes) interviennent durant les différentes étapes de la fabrication et de l'exploitation d'une carte à puce. Ainsi, les composants sont fournis et parfois en partie initialisés par des fabricants de composants électroniques sur une tranche de silicium. Cette phase correspond à l'étape de fabrication du composant. L'étape suivante est la phase d'encartage réalisée par le fabricant de carte à puce. Elle inclut l'isolement d'un composant de la tranche de silicium, la connexion dudit composant à un module (ou antenne), l'intégration de l'ensemble sur leur support ou corps de carte. Suit la préparation de la structure applicative présente dans la mémoire programmable électriquement du composant. C'est l'étape de personnalisation électrique qui est réalisée par le fabricant des cartes à puce ou par un centre de

personnalisation ou un tiers spécialisé dans la personnalisation des cartes ou par l'émetteur lui-même qui est chargé in fine de la distribution des cartes sur le marché. Cette phase de personnalisation électrique peut donc être décomposée en autant d'étapes qu'il y a acteurs ou d'intermédiaires. Par la suite, durant l'exploitation de la carte à puce, nous avons vu précédemment qu'il peut être intéressant de distinguer différentes étapes au gré de l'évolution du profil de l'utilisateur de la carte par exemple.

Quoi qu'il en soit, il est donc important de suivre rigoureusement les étapes de vie d'une carte pour connaître à tout moment l'étape en-cours de ladite carte au sein de son cycle de vie. De plus, il est indispensable que, d'une part, l'accès en écriture ou en lecture de la mémoire programmable électriquement du composant d'une carte soit protégé durant l'échange de ladite carte (ou du composant) entre les différents acteurs et que d'autre part l'accès à ladite mémoire soit limité au fur et à mesure que se succèdent les étapes de vie de la carte citées précédemment, en activant ou désactivant des services par exemple. Pour finir, il est également nécessaire parfois de valider le contexte applicatif de la carte à puce avant que le porteur de celle-ci l'utilise sur le marché. Par exemple, un émetteur de carte à puce de type porte-monnaie électronique, doit être certain que la balance de ladite carte est bien nulle avant d'émettre la carte.

Pour tenter de répondre à ces exigences, différentes solutions sont utilisées à ce jour. Certaines solutions sont purement extérieures à la carte à puce (sécurisation physique des locaux où ladite carte est fabriquée, utilisation de moyens de transport eux-mêmes sécurisés...). D'autres solutions complémentaires aux premières, mais cette fois internes ou implantées dans la carte, sont aussi

généralement utilisées. On utilise ainsi des secrets permettant de protéger l'accès en lecture/écriture de la mémoire du composant et également des indicateurs logiques permettant de suivre de manière irréversible les différentes étapes de vie de la carte. Pour cela, des bits au sein d'une mémoire non effaçable du composant de la carte à puce sont positionnés à l'état actif à la fin des différentes étapes de vie de la carte (fabrication et initialisation du composant par le fabricant dudit composant, encartage et initialisation de la mémoire de la carte par le fabricant de carte à puce, préparation de la structure applicative de la mémoire de la carte à puce par le centre de personnalisation ou l'émetteur de la carte...). En fonction de ces indicateurs, le programme (ou système d'exploitation), exécuté par le microprocesseur du composant de la carte à puce, implanté au sein de l'une des mémoires dudit composant de ladite carte, adapte son comportement au fur et à mesure que les étapes de vie de ladite carte se succèdent. Ainsi, des fonctions peuvent être modifiées, ajoutées ou supprimées.

Quelles que soient les solutions utilisées à ce jour, elles reposent toutes sur le fait que les différents acteurs impliqués dans la fabrication d'une carte sont des tiers de confiance. Seules des personnes, susceptibles d'intercepter des composants ou des cartes durant leur transfert entre deux des différents acteurs, sont supposées "fraudeurs potentiels" et les solutions exposées précédemment permettent de s'en affranchir. L'adaptation du système d'exploitation de la carte en fonction des indicateurs irréversibles apporte un plus non négligeable. Ainsi, si les fabricants de composants ou de cartes inscrivent des données systèmes ou des secrets, l'émetteur de la carte ne pourra par exemple librement s'affranchir desdits secrets ou modifier lesdites données système.

Cependant, cette solution ne résout pas le problème d'une initialisation frauduleuse de la carte ou d'une erreur malencontreuse durant ladite initialisation, effectuée par l'un des acteurs.

L'invention propose de remédier aux inconvénients de l'état actuel de la technique.

En particulier, l'invention consiste à doter le système d'exploitation d'une carte à puce de moyens logiciels permettant audit système d'exploitation de maîtriser un changement irréversible d'étape de vie de ladite carte en fonction d'un ensemble de vérifications du contenu des mémoires de cette même carte à puce. En outre l'invention prévoit que lors d'un changement d'étape de vie, le système d'exploitation de la carte puisse déclencher automatiquement des actions permettant d'adapter les services offerts par ledit système d'exploitation de ladite carte.

A cet effet, l'invention concerne un dispositif destiné à être implanté dans un objet électronique portatif, notamment une carte à puce, comprenant une unité de traitement, une mémoire volatile, des mémoires de programmes et des mémoires de données, le contenu desdites mémoires définissant une pluralité d'états qui correspondent respectivement à une configuration de l'objet électronique portatif, chacun desdits états déterminant les services offerts par ledit objet, caractérisé en ce qu'il comporte des moyens de contrôle de la transition d'un état à un autre état de l'objet électronique portatif.

Selon d'autres caractéristiques du dispositif selon l'invention :

- les moyens de contrôle comprennent des moyens de vérification de la cohérence du contenu des mémoires de données et/ou de programmes et/ou volatiles de l'objet

électronique portatif en fonction de la transition d'états à effectuer;

- les moyens de contrôle comprennent des moyens d'autorisation / interdiction des transitions d'état;
- les moyens de contrôle comprennent:
  - une table des transitions d'état possibles;
  - une table des vérifications à effectuer par transition d'état possible;
  - un moteur de vérification exploitant lesdites tables;
- les moyens de contrôle comprennent des moyens permettant de déclencher des actions lors du traitement d'une demande de franchissement d'une transition d'état;
- des actions, dites actions systématiques, sont déclenchées lors du franchissement d'une transition d'état ou du rejet du franchissement de ladite transition;
- des actions, dites actions positives, sont déclenchées lors du franchissement d'une transition d'état;
- des actions, dites actions négatives, sont déclenchées lors du rejet du franchissement d'une transition d'état;
- les moyens permettant de déclencher des actions, comprennent une table d'actions exploitable par le moteur de vérification;
- des états supplémentaires (dits états additifs) peuvent être ajoutés au sein de la mémoire de données;
- les moyens de contrôle de la transition d'état comprennent en outre au moins une extension de la table des transitions et au moins une extension de la table des vérifications, lesdites extensions de tables étant exploitables par le moteur de vérification;
- les moyens de contrôle de la transition d'état comprennent en outre au moins une extension de la table des actions, ladite extension de table étant exploitable par le moteur de vérification;

- la demande de transition peut être générée par une action déclenchée lors du franchissement ou du rejet de franchissement d'une transition;

En outre, l'invention concerne un procédé destiné à être exploité par un dispositif de contrôle du cycle de vie d'un objet électronique portatif comprenant une unité de traitement, une mémoire volatile, des mémoires de programmes et des mémoires de données, le contenu desdites mémoires définissant une pluralité d'états qui correspondent respectivement à une configuration donnée de l'objet, chacun desdits états déterminant les services offerts par ledit objet, caractérisé en que ledit procédé comprend une pluralité d'étapes, lesdites étapes étant dépendantes du type des états impliqués dans la demande de franchissement d'état appliquée à l'objet, le premier type d'état correspondant aux états prédéfinis dits "états de référence" et le second type d'état correspondant aux états pouvant être ajoutés dits "états additifs".

Selon d'autres caractéristiques du procédé, dans le cas où la demande de franchissement de transition appliquée à l'objet est une demande de franchissement de transition d'un état de référence vers un autre état de référence, ledit procédé comprend :

- une étape de validation de l'autorisation de ladite demande en analysant la table des transitions possibles;
- une étape d'évaluation des vérifications associées à la transition demandée en analysant la table des vérifications;
- une étape de modification de l'état courant de l'objet si et seulement si :
  - la transition demandée est autorisée
  - et, si les vérifications de la configuration de l'objet sont satisfaites;

- une étape d'exécution d'actions systématiques en analysant l'entrée de la table d'actions correspondant à la transition demandée;

- une étape d'exécution d'actions positives en analysant l'entrée de la table d'actions correspondant à la transition demandée si la transition demandée est autorisée et si les vérifications associées à la transition demandée sont satisfaites;

- une étape d'exécution d'actions négatives en analysant l'entrée de la table d'actions correspondant à la transition demandée si les vérifications associées à la transition demandée ne sont pas satisfaites.

Selon d'autres caractéristiques du procédé, dans le cas où la demande de franchissement de transition appliquée à l'objet est une demande de franchissement de transition d'un état additif vers un autre état additif, ledit procédé comprend :

- une étape de validation de l'autorisation de ladite demande en analysant une extension de la table des transitions possibles;

- une étape d'évaluation des vérifications associée à la transition demandée en analysant une extension de la table des vérifications;

- une étape de modification de l'état courant de l'objet si et seulement si :

  - la transition demandée est autorisée

  - et, si les vérifications de la configuration de l'objet sont satisfaites;

- une étape d'exécution d'actions systématiques en analysant l'entrée d'une extension de la table d'actions correspondant à la transition demandée;

- une étape d'exécution d'actions positives en analysant l'entrée d'une extension de la table d'actions correspondant à la transition demandée si la transition

demandée est autorisée et si les vérifications associées à la transition demandée sont satisfaites;

- une étape d'exécution d'actions négatives en analysant l'entrée d'une extension de la table d'actions correspondant à la transition demandée si les vérifications associées à la transition demandée ne sont pas satisfaites.

Selon d'autres caractéristiques du procédé, dans le cas où la demande de franchissement de transition appliquée à l'objet est une demande de franchissement de transition d'un état de référence vers un état additif, ledit procédé comprend :

- une étape de validation de l'autorisation d'une transition dudit état de référence vers un état additif en analysant la table des transitions possibles;
- une étape de validation de l'autorisation de la transition dudit état de référence vers ledit état additif en analysant une extension de la table des transitions possibles;
- une étape d'évaluation des vérifications associée à la transition demandée en analysant une extension de la table des vérifications;
- une étape de modification de l'état courant de l'objet si et seulement si :
  - la transition demandée est autorisée
  - et, si les vérifications de la configuration de l'objet sont satisfaites;
- une étape d'exécution d'actions systématiques en analysant l'entrée d'une extension de la table d'actions correspondant à la transition demandée;
- une étape d'exécution d'actions positives en analysant l'entrée d'une extension de la table d'actions correspondant à la transition demandée si la transition demandée est autorisée et si les vérifications associées à la transition demandée sont satisfaites;

- une étape d'exécution d'actions négatives en analysant l'entrée d'une extension de la table d'actions correspondant à la transition demandée si les vérifications associées à la transition demandée ne sont pas satisfaites.

Selon d'autres caractéristiques du procédé, dans le cas où la demande de franchissement de transition appliquée à l'objet est une demande de franchissement de transition d'un état additif vers un état de référence, ledit procédé rejette ladite demande.

L'invention concerne également un objet électronique portatif, comportant une unité de traitement, une mémoire volatile, des mémoires de programmes et des mémoires de données, caractérisé en ce qu'il comporte ledit dispositif de contrôle du cycle de vie de l'objet.

En outre, l'invention concerne une carte à puce, comportant une unité de traitement, une mémoire volatile, des mémoires de programmes et des mémoires de données, caractérisé en ce qu'elle comporte ledit dispositif de contrôle du cycle de vie de la carte.

L'invention sera mieux comprise à la lecture de la description qui suit et à l'examen des figures qui l'accompagnent. Celles-ci ne sont données qu'à titre indicatif et nullement limitatif de l'invention. Les figures montrent:

- figure 1: un composant d'une carte à puce munie d'un dispositif de vérification de transition d'état;
- figures 2a et 2b: une représentation détaillée d'une table des transitions d'état;
- figure 3: une représentation détaillée d'une table des vérifications des transitions;
- figure 4: une représentation détaillée d'une table des actions;

- figure 5: une description des étapes mises en ouvre dans le procédé utilisé par le dispositif de vérification de transitions;

- figures 6a à 6d: les particularités mises en oeuvre dans le cas d'un exemple d'une carte à puce de type porte-monnaie électronique;

Dans l'invention, on appellera état de référence, un état à partir duquel il est possible de basculer vers un autre état suite au franchissement d'une transition décrite dans la table des transitions, implantée dans la mémoire de programme. Comme il est décrit plus loin, il est possible d'ajouter de nouveaux états et donc de nouvelles transitions après que l'étape de fabrication du composant ait eu lieu. Dans ce cas, on parlera d'états additifs pour caractériser ceux-ci par opposition aux états de référence. D'autre part, on appellera état courant l'état dans lequel se trouve le système embarqué.

La figure 1 montre un composant 1, d'une carte à puce, muni d'un dispositif de vérification de transitions selon l'invention. Le composant comporte une unité de traitement 2 ou encore microprocesseur en relation avec des mémoires 3, 4 et 5 via un bus de communication 6. Une mémoire de programme 4 (ou encore ROM) non effaçable comporte d'une part une zone de programmes 7, lesdits programmes (ou encore système d'exploitation du système embarqué) pouvant être exécutés par ladite unité de traitement et d'autre part une zone de données pré-définies 10 qui contient des constantes utilisées par ledit système d'exploitation. Parmi lesdites constantes de la zone 10, le système d'exploitation 7, comportant un programme appelé moteur de vérification 9, exploite une table des transitions 11 qui permet de préciser les états auxquels on peut accéder à partir de l'état courant, une table des vérifications 12 qui permet d'associer à chaque transition d'état des vérifications portant sur le contenu des mémoires 3, 4

et/ou 5. Dans une variante, le moteur de vérification 9 peut déclencher automatiquement des actions lors du franchissement ou du rejet du franchissement d'une transition. Pour cela la zone 10 de la mémoire de programme comporte une table des actions 13 qui permet d'associer à chaque transition d'état possible des actions à effectuer.

Une mémoire volatile 3 (ou encore RAM pour Random Access Memory en langue anglaise) permet à l'unité de traitement 2 de stocker de manière temporaire des résultats ou encore des secrets issus de calculs décrits par les programmes implantés dans la mémoire de programme 4. Le contenu de la mémoire 3 est effacé à chaque mise sous tension du composant 1 ou à chaque demande de remise à zéro de celui-ci.

Une mémoire de données 5, effaçable électriquement utilisant généralement la technologie EEPROM (pour Electrical Erasable Programmable Read Only Memory en langue anglaise) comporte une zone 14 contenant les données variables nécessaires à l'exécution des programmes 7. Cette zone 14 comporte notamment une donnée 8 appelée "Etat courant" permettant de mémoriser l'état courant de l'objet électronique portatif. La mémoire de données 5 comporte en outre une zone 15 comprenant optionnellement des extensions des tables 11 à 13 dans le cas où il est nécessaire d'ajouter des états aux états de références. La zone 15 comporte alors une extension de la table des transitions 16, une extension de la table des vérifications 17 et peut comporter une extension de la table des actions 18 si l'on souhaite associer aux nouvelles transitons d'état additif des actions, comme vu précédemment pour ce qui concerne la table 13. Dans le cas d'ajout d'états par rapport aux états de référence, il est parfois indispensable d'enrichir le système d'exploitation 7. Pour cela, la mémoire 5 peut comporter en outre une zone 19 qui contient les programmes

supplémentaires qui seront exécutés à leur tour par l'unité de traitement 2.

La figure 2a montre une mise en ouvre possible de la table des transitions 11. Si l'on suppose que l'on dénombre i états de référence, on peut imaginer une table de transition comprenant i colonnes et i lignes. Les colonnes correspondent aux états de référence pouvant être, à un instant donné, l'état courant. Les i premières lignes correspondent aux états de référence auxquels on peut accéder à partir de l'état courant. Ainsi la valeur d'une case de la table des transitions 11 correspondant à l'intersection d'une ligne et d'une colonne de ladite table permet de coder soit, l'absence de transition autorisée (valeur nulle par exemple - c'est le cas de la transition 20), soit, l'autorisation une transition (valeur non nulle - c'est le cas de la transition 21). Dans le cas d'une transition autorisée, le moteur de vérification de transitions recherche au sein de la table de vérification 12 les vérifications à effectuer pour accepter ou rejeter le franchissement de la transition demandée.

La figure 2b montre également une mise en ouvre possible d'une table de transition dans le cas où il est possible d'ajouter des états (états additifs) aux états de référence. La table des transitions comporte une ligne supplémentaire par rapport à la figure 2a. La (i+1)ème ligne permet de préciser si l'on autorise des transitions d'un état de référence courant à un état additif. Ainsi la valeur de la case 22 indique une transition interdite d'un état de référence vers un état additif. La case 23 indique qu'il sera possible de basculer de l'état de référence Ei vers un état additif. Une extension 16 de la table des transitions est alors nécessaire. Cette dernière comporte j lignes correspondant à j états additifs auxquels on peut accéder à partir de (i+j) états courant possibles matérialisés par les (i+j) colonnes de l'extension 16 de la

table des transitions. Ainsi la combinaison de la case 23 de la table des transitions et de la case 24 de l'extension 16 de la table des transitions, indique au moteur de vérification qu'il est possible de basculer de l'état de référence Ei vers l'état additif E(i+1).

La figure 3 montre une mise en ouvre de la table des vérifications. La table des vérifications 12 est implantée au sein de la zone 10 des données pré-définies de la mémoire 4. Chaque transition autorisée dispose d'une entrée dans ladite table. Une entrée comprend un champ 30 permettant d'identifier la transition et un champ 31 contenant une référence (ou adresse) vers un programme 32 du système d'exploitation 7. Le moteur de vérification 9 peut ainsi faire exécuter à l'unité de traitement 2 les contrôles requis pour accepter le franchissement de la transition. La figure 3 illustre également une structure d'une extension 17 de la table des vérifications. De la même manière que pour la table 12, l'extension de la table des vérifications 17 comporte une entrée par transition possible. Chaque entrée comprend deux champs, un champ 33 permettant d'identifier la transition et un champ 34 contenant une référence (ou adresse) d'un programme 35 du système d'exploitation ou, comme le montre la figure 3, d'un programme supplémentaire implanté dans la mémoire de données 5 (en zone 19).

La figure 4 montre une représentation de la table des actions 13 implantée dans la zone 10 des données pré-définies de la mémoire de programmes 4. Lors d'une demande de franchissement de transition, il est possible de déclencher des actions. Celles-ci peuvent être de trois types: action systématique, action positive (c'est à dire conditionnée au fait que les vérifications sont satisfaisantes) ou action négative (c'est à dire conditionnée au fait que les vérifications ne sont pas satisfaisantes). La figure 4 montre qu'à chaque transition

autorisée, il existe une entrée dans la table des actions 13. Cette entrée comprend 4 champs. Le premier champ 400 permet d'identifier la transition. Les trois autres champs 401, 402 et 403 contiennent chacun une référence ou adresse d'un programme 404, 405 ou 406 du système d'exploitation. Le champ 401 est dédié à une action systématique, le champ 402 à une action positive et le champ 403 à une action négative. La figure 4 montre également une extension 18 de la table des actions. Cette table 18 est implantée dans la zone 15 de la mémoire de données 5 du composant 1. De la même manière que pour la table des actions 13, l'extension de la table des actions 18 comprend une entrée par transition possible. Une entrée comprend 4 champs. Le premier champ 407 permet d'identifier la transition. Les trois autres champs 408, 409 et 410 contiennent chacun une référence ou adresse d'un programme 411, 412 ou 413 du système d'exploitation ou comme le montre la figure 4, des programmes implantés dans la zone 19 de la mémoire de données 5 du composant 1. Le champ 408 est dédié à une action systématique, le champ 409 à une action positive et le champ 410 à une action négative.

La figure 5a décrit le procédé permettant de valider ou de rejeter le franchissement d'une transition d'état, d'un premier état de référence vers un autre état de référence. La demande de franchissement d'une transition peut être formulée suite à un ordre du fabricant de carte ou par tout autre acteur du cycle de vie de la carte à puce. Ladite demande peut également être formulée directement par la carte-elle même, par exemple au travers d'une action associée à une transition. Dans le cadre de la figure 5a, l'état de référence courant est l'état Ei. L'ordre 50 de basculement de l'état Ei à l'état Ej est formulé. L'étape 51 consiste à vérifier au sein de la table des transitions 11 que la transition de l'état Ei vers l'état Ej est autorisée. Dans le cas où cette transition est interdite,

la demande de franchissement de transition 50 est rejetée. L'état courant demeure l'état Ei. Par contre, si la transition est autorisée, le moteur de vérification 9 exécute les vérifications associées à ladite transition. Pour cela le moteur de vérification évalue l'entrée de la table des vérifications 12 dédiée à la transition T(Ei->Ej). L'exécution desdites vérifications correspond à l'étape 52 du procédé. Le moteur de vérification 9 exécute les actions systématiques associées à la transition T(Ei->Ej) en fonction de l'entrée de la table des actions 13 dédiées à ladite transition (étape 53). Si les vérifications 54 exigées lors de la demande de franchissement de la transition 50 sont non satisfaisantes, l'état courant demeure inchangé. En fonction de l'entrée de la table des actions 13 associée à la transition T(Ei->Ej) le moteur de vérifications exécute les actions négatives (étape 55 du procédé). Le déroulement du procédé est alors terminé. Par contre, si les vérifications 54 sont satisfaisante, alors l'état courant devient l'état Ej (étape 56 du procédé). Les actions positives sont alors exécutées (étape 57 du procédé) en fonction de l'état de l'entrée de la table des actions 13 associée à la transition T(Ei->Ej). Le déroulement du procédé est terminé.

La figure 5b décrit le procédé permettant de valider ou de rejeter le franchissement d'une transition d'état, d'un premier état additif vers un autre état additif. L'état additif courant est l'état Ei. L'ordre 510 de basculer de l'état additif Ei à l'état additif (ou de référence) Ej est formulé. L'étape 511 du procédé consiste à vérifier au sein de l'extension la table des transitions 16 que la transition de l'état Ei à l'état Ej est autorisée. Dans le cas où cette transition est interdite, la demande de franchissement de transition 510 est rejetée. L'état courant demeure l'état Ei. Par contre, si la transition est

autorisée, le moteur de vérification 9 exécute les vérifications associées à ladite transition. Pour cela, le moteur de vérification évalue l'entrée de l'extension de la table des vérifications 17 dédiée à la transition T(Ei->Ej). L'exécution desdites vérifications constitue l'étape 512 du procédé. Le moteur de vérification 9 exécute les actions systématiques associées à la transition T(Ei->Ej) en fonction de l'entrée de l'extension de la table des actions 18 dédiées à ladite transition (étape 513 du procédé). Si la vérification 514 exigée lors de la demande de franchissement de la transition 510 est non satisfaisante, l'état courant demeure inchangé. En fonction de l'entrée de l'extension de la table des actions 18 associée à la transition T(Ei->Ej), le moteur de vérification 9 exécute les actions négatives (étape 515 du procédé). Le déroulement du procédé est alors terminé. Par contre, si les vérifications 514 sont satisfaisantes, l'état courant devient l'état Ej (étape 516 du procédé). Les actions positives sont alors exécutées (étape 517 du procédé) en fonction de l'état de l'entrée de l'extension de la table des actions 18 associée à la transition T(Ei->Ej). Le déroulement du procédé est terminé.

La figure 5c décrit le procédé permettant de valider ou de rejeter le franchissement d'une transition d'état, d'un état de référence vers un état additif. L'état de référence courant est l'état Ei. L'ordre 520 de basculement de l'état de référence Ei à l'état additif Ej est formulé. L'étape 528 du procédé consiste à vérifier au sein de la table des transitions 11, qu'une transition de l'état de référence courant Ei vers un état additif est autorisée. Si une telle transition est interdite, le procédé est terminé. L'état courant demeure inchangé. Par contre, si une transition dudit état de référence vers un état additif est autorisée, le moteur de vérification déroule les étapes 521 à 527 du

procédé, respectivement identiques aux étapes 511 à 517 décrites en liaison avec la figure 5b.

Un exemple d'application dans le domaine du Porte-monnaie électronique est présenté en liaison avec les figures 6a à 6d. Ladite application permet de régler des achats à l'aide "d'argent électronique" stocké dans une carte à puce, au lieu de payer en numéraire. L'emploi d'une telle technique impose une gestion des cartes aussi sécurisée que celle qu'aurait imposé l'emploi du numéraire. Il faut par exemple éviter la création de monnaie fictive. La sécurité d'une carte à puce porte-monnaie électronique repose généralement sur des clés stockées à l'intérieur de ladite carte à puce permettant des transactions sécurisées en utilisant la cryptographie. Une telle carte dispose d'un système d'exploitation offrant un jeu de commandes et de services permettant de créditer ou de débiter de l'argent. Au début du cycle de vie de la carte à puce porte-monnaie électronique, ladite carte à puce n'est pas initialisée. Elle ne contient aucune information. La figure 6a montre les états de référence pré-définis :

- Etat E1 "carte vierge" (référencé 80): seules des commandes de test permettant de valider le comportement de la mémoire de données 5 sont disponibles (vérification que les cases mémoires de technologie EEPROM peuvent être correctement écrites et effacées);

- Etat E2 "carte testée" (référencé 82): Les commandes de test ne sont plus disponibles. A leur tour des commandes dites généralement "commandes physiques" (permettant un accès en écriture par un adressage physique indépendamment de toute structure logique de type fichier par exemple) sont disponibles. Elles permettent d'initialiser la carte (écriture dans la zone 14 de la mémoire de données des constituants logiques nécessaires au fonctionnement de l'application c'est à dire fichiers, balances...);

- Etat E3 "carte initialisée" (référencé 84): les commandes physiques ne sont plus disponibles. Des commandes logiques permettent de personnaliser la carte (ajout de nouvelles structures logiques et initialisation de données dans lesdites structures) sont utilisables. En outre, un mécanisme de recouvrement est activé de sorte que la carte à puce ne perde pas la cohérence de ces données lors d'une mise hors tension de celle-ci durant l'exécution de l'une desdites commandes logiques.

- Etat E4 "carte personnalisée" (référencé 86): les commandes logiques spécifiques à l'application Porte-monnaie électronique (débit/crédit) sont activées.

Le jeu de commandes disponibles évolue en fonction de l'étape de vie dans laquelle se trouve la carte à puce. Des informations stockées en mémoire de données permettent au système d'exploitation de connaître l'état dans lequel la carte à puce se trouve. La figure 6a montre en outre que dans le cadre d'une carte de type porte-monnaie électronique, toutes les transitions entre états de référence doivent être franchies successivement (de l'état E1 à l'état E4) et ce de manière irréversible. Toute autre transition est interdite. Seule la possibilité d'utiliser ultérieurement des états additifs 88 est offerte. Cette transition possible est référencée 87. Le système d'exploitation en fonction de l'état courant n'autorise qu'un ensemble de commandes spécifiques à chaque état de référence.

Les vérifications et les actions à déclencher lors du franchissement d'une transition sont décrites comme suit :

- Transition de l'état E1 vers l'état E2 (notée T(E1->E2) et référencée 81) :
  - Vérification: aucune
  - Action systématique :
    effacement de la mémoire de données pour éviter qu'un fraudeur y laisse des données

interprétables par le système d'exploitation de la carte;

- Transition de l'état E2 vers l'état E3 (notée T(E2->E3) et référencée 83) :
  - Vérification:
    - intégrité des données écrites dans la mémoire de données avec les commandes physiques (validation d'un code de redondance par donnée);
    - vérification de l'état vierge de la mémoire en dehors desdites données;
  - Action positive :
    - activation du mécanisme de recouvrement;
- Transition de l'état E3 vers l'état E4 (notée T(E3->E4) et référencée 85) :
  - Vérification:
    - nullité de la balance du porte monnaie électronique
  - Action : aucune
- Transition de l'état E4 vers un état additif (notée T(E4->Eadd) et référencée 87) :
  - Vérification : aucune
  - Action : aucune

Les figures 6b à 6d illustrent respectivement une réalisation d'une table des transitions 11, d'une table des vérifications 12 et d'une table d'actions 13, selon l'invention. La table des transitions 11 telle que décrite en liaison avec la figure 6b permet de n'autoriser que les transitions 81, 83, 85 et 87. Pour cela seules les cases 60 à 63 de ladite table contiennent une valeur non nulle. Les autres cases de la table des transitions contiennent une valeur nulle pour indiquer que toute autre transition est interdite. La table des vérifications telle que présentée au travers de la figure 6c, permet d'associer les vérifications à satisfaire pour autoriser le franchissement

des transitions 81, 83, 85 et 87, lesdites transitions autorisées par la table des transitions 11 (figure 6b). Ainsi l'entrée 64 de la table des vérifications 12 comporte un champ 641 permettant d'identifier que ladite entrée est dédiée à la transition 81. L'entrée 64 comporte en outre un champ 642 contenant une référence nulle pour indiquer qu'aucune vérification n'est demandée pour autoriser le franchissement de la transition 81. Dans une variante, la transition 81 ne dispose d'aucune entrée associée. Cette variante est illustrée plus loin dans le cas de la table des actions. La table des vérifications 12 comporte une entrée 65 qui comprend respectivement un champ 651 pour indiquer que l'entrée est associée à la transition 83 et un champ 652 contenant la référence d'un programme 67, implanté dans la mémoire de programmes, pour que le moteur de vérification puisse effectuer les vérifications décrites précédemment. De même, la table des vérifications 12 comporte une entrée 66 qui comprend respectivement un champ 661 pour indiquer que l'entrée est associée à la transition 83 et un champ 662 contenant la référence d'un programme 68, implanté dans la mémoire de programmes, pour que le moteur de vérification puisse effectuer les vérifications décrites précédemment.

La figure 6d présente une réalisation de la table des actions 13. Ladite table comporte une entrée 71 qui comporte un champ 711 permettant d'indiquer que ladite entrée est associée à la transition 81. La même entrée 71 comporte un champ 712 contenant la référence d'un programme 75, implanté dans la mémoire de programmes, afin que le moteur de vérification puisse exécuter les actions systématiques associées à la transition 81. L'entrée 71 comporte en outre un champ 713 et un champ 714 contenant une référence nulle pour indiquer au moteur de vérification qu'aucune action positive ni négative n'est associée au franchissement de la transition 81. De la même manière, la

table des actions 13 comporte une seconde entrée 72 comprenant les champs 721 à 724 pour indiquer au moteur de vérification que ladite entrée est associée à la transition 83, que le programme 74 est à exécuter comme action positive lors du franchissement de ladite transition et qu'aucune action systématique ou négative n'est à exécuter. L'absence d'entrée, au sein de la table des actions 13, associée à la transition 85, indique qu'aucune action (systématique, positive ou négative) n'est à exécuter lors du franchissement ou du rejet du franchissement de ladite transition.

Grâce au dispositif et au procédé tels que décrits ci-dessus, le cycle de vie d'un objet électronique portatif est maîtrisé. Chaque transition d'états est irréversible et les vérifications faites lors de chaque demande de transitions garantissent une configuration mémoire de l'objet cohérente. En outre les actions systématiques, positives ou négatives permettent d'adapter le comportement dudit objet. Enfin, dans le cas où il est prévu d'autoriser une ou plusieurs transitions d'un ou plusieurs états de référence vers un état additif, le cycle de vie de l'objet peut être facilement enrichi, par exemple après que l'objet soit émis sur le marché, sans que le cycle de vie prédéfini (composé par une succession de transitions d'état de référence vers un autre état de référence) puisse être détourné.

Tout risque de fraude durant l'initialisation d'un objet électronique portatif ou d'erreur malencontreuse durant ladite initialisation est écarté tout en conservant grande adaptabilité du contrôle du cycle de vie de l'objet.

## REVENDICATIONS

1. Dispositif de contrôle du cycle de vie, destiné à être implanté dans un objet électronique portatif comprenant une unité de traitement (2), une mémoire volatile (3), des mémoires de programmes (4) et des mémoires de données (5), le contenu desdites mémoires définissant une pluralité d'états qui correspondent respectivement à une configuration donnée de l'objet, chacun desdits états déterminant les services offerts par ledit objet, caractérisé en ce qu'il comporte des moyens de contrôle de la transition d'un état à un autre état de l'objet électronique portatif.

2. Dispositif selon la revendication 1, caractérisé en ce que les moyens de contrôle comprennent des moyens de vérification de la cohérence du contenu de la mémoire volatile, des mémoires de données et des mémoires de programmes de l'objet électronique portatif en fonction de la transition d'états à effectuer.

3. Dispositif selon l'une quelconque des revendications 1 ou 2, caractérisé en ce que les moyens de contrôle comportent des moyens d'autorisation et/ou interdiction des transitions d'état.

4. Dispositif selon l'une quelconque des revendications 1 à 3, caractérisé en ce que les moyens de contrôle comprennent:

- une table (11) des transitions d'état possibles;
- une table (12) des vérifications à effectuer par transition d'état possible;
- un moteur de vérification (9) exploitant lesdites tables.

5. Dispositif selon l'une quelconque des revendications 1 à 4, caractérisé en ce qu'il comprend des moyens permettant de déclencher des actions lors du traitement d'une demande de franchissement de transition d'un état à un autre état de l'objet électronique portatif.

6. Dispositif selon l'une quelconque des revendications 1 à 5, caractérisé en ce que des actions, dites actions systématiques, sont déclenchées lors du franchissement d'une transition ou du rejet du franchissement d'une transition.

7. Dispositif selon l'une quelconque des revendications 1 à 6, caractérisé en ce que des actions, dites actions positives, sont déclenchées lors du franchissement d'une transition.

8. Dispositif selon l'une quelconque des revendications 1 à 7, caractérisé en ce que des actions, dites actions négatives, sont déclenchées lors du rejet de franchissement d'une transition.

9. Dispositif selon l'une quelconque des revendications 1 à 8, caractérisé en ce que les moyens permettant de déclencher des actions lors du traitement d'une demande de franchissement de transition d'un état à un autre état de l'objet électronique portatif, comprennent une table (13) d'actions exploitable par ledit moteur de vérification (9).

10. Dispositif selon l'une quelconque des revendications 1 à 9, caractérisé en ce que des états supplémentaires (dits états additifs) peuvent être ajoutés au sein de la mémoire de données.

11. Dispositif selon la revendication 10, caractérisé en ce que les moyens de contrôle de la transition d'un état à un autre état de l'objet électronique portatif comprennent en outre au moins:

- une extension (16) de la table (11) des transitions d'état possibles;

- une extension (17) de la table (12) des vérifications à effectuer par transition d'état possible;

et en ce que le moteur de vérification (9) exploite lesdites extensions de tables (16, 17).

12. Dispositif selon l'une quelconque des revendications 10 ou 11, caractérisé en ce que les moyens permettant de déclencher des actions lors du traitement d'une demande de franchissement de transition d'un état à un autre état de l'objet électronique portatif, comprennent au moins une extension (18) de la table (13) d'actions exploitable par le moteur de vérification (9).

13. Dispositif selon l'une quelconque des revendications 1 à 12, caractérisé en ce que la demande de transition peut être générée par une action déclenchée lors du franchissement ou du rejet du franchissement d'une transition.

14. Objet électronique portatif, comportant une unité de traitement (2), une mémoire volatile (3), des mémoires de programmes (4) et des mémoires de données (5), caractérisé en ce qu'il comporte le dispositif de contrôle du cycle de vie de l'objet, selon l'une des revendications 1 à 13.

15. Carte à puce, comportant une unité de traitement (2), une mémoire volatile (3), des mémoires de programmes (4) et des mémoires de données (5), caractérisé en ce qu'elle

comporte le dispositif de contrôle du cycle de vie de la carte, selon l'une des revendications 1 à 13.

16. Procédé, destiné à être exploité par un dispositif de contrôle du cycle de vie d'un objet électronique portatif comprenant une unité de traitement (2), une mémoire volatile (3), des mémoires de programmes (4) et des mémoires de données (5), le contenu desdites mémoires définissant une pluralité d'états qui correspondent respectivement à une configuration donnée de l'objet, chacun desdits états déterminant les services offerts par ledit objet,

caractérisé en qu'il comporte une pluralité d'étapes, lesdites étapes étant dépendantes du type des états impliqués dans la demande de franchissement d'état appliquée à l'objet, le premier type d'état correspondant aux états prédéfinis dans la mémoire de programmes (4), dits "états de référence" et, le second type d'état correspondant aux états pouvant être ajoutés dans la mémoire de données (5), dits "états additifs".

17. Procédé selon la revendication 16, pour lequel la demande de franchissement de transition appliquée à l'objet est une demande de franchissement de transition d'un état de référence vers un autre état de référence, caractérisé en que ledit procédé comprend au moins :

- une étape (51) de validation de l'autorisation de ladite demande en analysant la table (11) des transitions possibles;
- une étape (52) d'évaluation des vérifications associée à la transition demandée en analysant une table (12) des vérifications;
- une étape (57) de modification de l'état courant de l'objet si et seulement si :
  - la transition demandée est autorisée (51)

- et, si les vérifications de la configuration de l'objet sont satisfaites (54).

18. Procédé selon l'une quelconque de la revendication 17, caractérisé en ce qu'il comprend en outre une étape (53) d'exécution d'actions systématiques en analysant l'entrée de la table (13) d'actions correspondant à la transition demandée.

19. Procédé selon l'une quelconque des revendications 17 ou 18, caractérisé en ce qu'il comprend en outre une étape (56) d'exécution d'actions positives en analysant l'entrée de la table (13) d'actions correspondant à la transition demandée dans le cas où la transition demandée est autorisée (51) et si les vérifications associées à la transition demandée sont satisfaites (54).

20. Procédé selon l'une quelconque des revendications 17 à 19, caractérisé en ce qu'il comprend en outre une étape (55) d'exécution d'actions négatives en analysant l'entrée de la table (13) d'actions correspondant à la transition demandée dans le cas où les vérifications associées à la transition demandée ne sont pas satisfaites (54).

21. Procédé selon la revendication 16, pour lequel la demande de franchissement de transition appliquée à l'objet est une demande de franchissement de transition d'un état additif vers un autre état additif, caractérisé en ce qu'il comprend au moins:

- une étape (511) de validation de l'autorisation de ladite demande en analysant une extension (16) de la table (11) des transitions possibles;

- une étape (512) d'évaluation des vérifications associée à la transition demandée en analysant une extension (17) de la table (12) des vérifications;

- une étape (517) de modification de l'état courant de l'objet si et seulement si :

- la transition demandée est autorisée (511)

- et, si les vérifications de la configuration de l'objet sont satisfaites (514).

22. Procédé selon la revendication 21, caractérisé en ce qu'il comprend en outre une étape (513) d'exécution d'actions systématiques en analysant l'entrée d'une extension (18) de la table (13) d'actions correspondant à la transition demandée.

23. Procédé selon l'une quelconque des revendications 21 ou 22, caractérisé en ce qu'il comprend en outre une étape (516) d'exécution d'actions positives en analysant l'entrée de l'extension (18) de la table (13) d'actions correspondant à la transition demandée si :

- la transition demandée est autorisée (511)

- et, si les vérifications associées à la transition demandée sont satisfaites (514).

24. Procédé selon l'une quelconque des revendications 22 à 23, caractérisé en ce qu'il comprend en outre une étape (515) d'exécution d'actions négatives en analysant l'entrée d'une extension (18) de la table (13) d'actions correspondant à la transition demandée dans le cas où les vérifications associées à la transition demandée ne sont pas satisfaites (514).

25. Procédé selon la revendication 16, pour lequel la demande de franchissement de transition appliquée à l'objet

est une demande de franchissement de transition d'un état de référence vers un état additif, caractérisé en ce qu'il comprend au moins:

- une étape (528) de validation de l'autorisation de d'une transition dudit état de référence vers un état additif en analysant la table (11) des transitions possibles;
- une étape (521) de validation de l'autorisation de d'une transition dudit état de référence vers ledit état additif en analysant une extension (16) de la table (11) des transitions possibles;
- une troisième étape (522) d'évaluation des vérifications associée à la transition demandée en analysant une extension (17) d'une table (12) des vérifications;
- une étape (527) de modification de l'état courant de l'objet si et seulement si :
  - la transition demandée est autorisée (528, 521)
  - et, si les vérifications de la configuration de l'objet sont satisfaites (524).

26. Procédé selon la revendication 25, caractérisé en ce qu'il comprend en outre une étape (523) d'exécution d'actions systématiques en analysant l'entrée d'une extension (18) de la table (13) d'actions correspondant à la transition demandée.

27. Procédé selon l'une quelconque des revendications 25 ou 26, caractérisé en ce qu'il comprend en outre une étape (526) d'exécution d'actions positives en analysant l'entrée d'une extension (18) de la table (13) d'actions correspondant à la transition demandée si :

- la transition demandée est autorisée (528, 521)
- et, si les vérifications associées à la transition demandée sont satisfaites (524).

28. Procédé selon l'une quelconque des revendications 25 à 27, caractérisé en ce qu'il comprend en outre une étape (525) d'exécution d'actions négatives en analysant l'entrée d'une extension (18) de la table (13) d'actions correspondant à la transition demandée dans le cas où les vérifications associées à la transition demandée ne sont pas satisfaites (524).

29. Procédé selon l'une quelconque des revendications 16 à 28, caractérisé en ce que ledit procédé n'autorise pas le franchissement d'une transition d'état, d'un état additif vers un état de référence.

**REVENDICATIONS**

1. Dispositif de contrôle du cycle de vie d'un objet électronique portatif, le cycle de vie étant déterminé par une succession de transitions d'états, lesdits états déterminant les services offerts par l'objet, ledit objet comprenant une unité de traitement (2), une mémoire volatile (3), des mémoires de programmes (4) et des mémoires de données (5), chacune de ces mémoires (3, 4, 5) présentant un contenu définissant une pluralité de configurations,

caractérisé en ce qu'il comporte des moyens de contrôle de la transition d'un premier état à un second état de l'objet électronique portatif.

2. Dispositif selon la revendications 1, caractérisé en ce que les moyens de contrôle comportent des moyens d'autorisation et/ou interdiction de transitions d'état.

3. Dispositif selon l'une quelconque des revendications 1 ou 2, caractérisé en ce que les moyens de contrôle comprennent des moyens de vérification du contenu de la mémoire volatile (3), des mémoires de données (5) et des mémoires de programmes (4) de l'objet électronique portatif en fonction de la transition d'états à effectuer.

4. Dispositif selon l'une quelconque des revendications 1 à 3, caractérisé en ce que les moyens de contrôle comprennent:

- une table (11) des transitions d'état possibles;
- une table (12) des vérifications à effectuer par transition d'état possible;
- un moteur de vérification (9) exploitant lesdites tables.

5. Dispositif selon l'une quelconque des revendications 1 à 4, caractérisé en ce que les moyens de contrôle comprennent en outre des moyens permettant de déclencher des actions lors du traitement d'une demande de franchissement de transition d'un premier état à un second état de l'objet électronique portatif.

6. Dispositif selon la revendication 5, caractérisé en ce que les moyens permettant de déclencher des actions lors du traitement d'une demande de franchissement de transition d'un premier état à un second état de l'objet électronique portatif, comprennent une table (13) d'actions exploitable par ledit moteur de vérification (9).

7. Dispositif selon l'une quelconque des revendications 1 à 6, caractérisé en ce que les moyens de contrôle de la transition d'un premier état à un second état de l'objet électronique portatif comprennent en outre :

- une extension (16) de la table (11) des transitions d'état possibles;
- une extension (17) de la table (12) des vérifications à effectuer par transition d'état possible;

et en ce que le moteur de vérification (9) exploite lesdites extensions de tables (16, 17).

8. Dispositif selon l'une quelconque des revendications 5 à 7, caractérisé en ce que les moyens permettant de déclencher des actions lors du traitement d'une demande de franchissement de transition d'un premier état à un second état de l'objet électronique portatif, comprennent en outre une extension (18) de la table (13) d'actions exploitable par le moteur de vérification (9).

9. Objet électronique portatif, comportant une unité de traitement (2), une mémoire volatile (3), des mémoires de programmes (4) et des mémoires de données (5), caractérisé en ce qu'il comporte le dispositif de contrôle du cycle de vie de l'objet, selon l'une des revendications 1 à 8.

10. Carte à puce, comportant une unité de traitement (2), une mémoire volatile (3), des mémoires de programmes (4) et des mémoires de données (5), caractérisé en ce qu'elle comporte le dispositif de contrôle du cycle de vie de la carte, selon l'une des revendications 1 à 8.

11. Procédé de contrôle du cycle de vie d'un objet électronique portatif, le cycle de vie étant déterminé par une succession de transitions d'états, lesdits états déterminant les services offerts par l'objet, ledit objet comprenant une unité de traitement (2), une mémoire volatile (3), des mémoires de programmes (4) et des mémoires de données (5), chacune de ces mémoires (3, 4, 5) présentant un contenu définissant une pluralité de configurations,

ledit procédé étant mis en oeuvre, au sein de l'objet, à la suite d'une demande de transition d'états,

caractérisé en qu'il comprend :

- une étape (51, 511, 528, 521) de validation de l'autorisation de ladite demande;
- une étape (52, 512, 522) d'évaluation des vérifications associée à la transition demandée;
- une étape (57, 517, 527) de modification de l'état courant de l'objet si et seulement si la transition demandée est autorisée (51, 511, 528, 521) et, si les vérifications de la configuration de l'objet sont satisfaites (54, 514, 524).

12. Procédé selon la revendication 11, caractérisé en ce qu'il comprend en outre une étape (53, 513, 523) d'exécution d'actions systématiques.

13. Procédé selon l'une quelconque des revendications 11 ou 12 , caractérisé en ce qu'il comprend en outre une étape (56, 516, 526) d'exécution d'actions positives dans le cas où la transition demandée est autorisée (51, 511, 528, 521) et si les vérifications associées à la transition demandée sont satisfaites (54, 514, 524).

14. Procédé selon l'une quelconque des revendications 11 à 13, caractérisé en ce qu'il comprend en outre une étape (55, 515, 525) d'exécution d'actions négatives dans le cas où les vérifications associées à la transition demandée ne sont pas satisfaites (54, 514, 524).

15. Procédé selon l'une quelconque des revendications 11 à 14, mis en oeuvre au sein de l'objet, à la suite d'une demande de transition d'un premier état de référence vers un second état de référence, caractérisé en qu'il comprend :

- une étape (51) de validation de l'autorisation de ladite demande consistant à analyser la table (11) des transitions possibles;
- une étape (52) d'évaluation des vérifications associée à la transition demandée consistant à exploiter une entrée (30) d'une table (12) des vérifications;
- une étape (57) de modification de l'état courant de l'objet si et seulement si la transition demandée est autorisée (51) et, si les vérifications de la configuration de l'objet sont satisfaites (54).

16. Procédé selon la revendication 15, caractérisé en ce qu'il comprend en outre une étape (53) d'exécution d'actions systématiques consistant à exploiter une entrée (400, 401, 404), correspondant à la transition demandée, d'une table (13) d'actions.

17. Procédé selon l'une quelconque des revendications 15 ou 16 , caractérisé en ce qu'il comprend en outre une étape (56) d'exécution d'actions positives consistant à exploiter une entrée (400, 402, 405), correspondant à la transition demandée, d'une table (13) d'actions, dans le cas où la transition demandée est autorisée (51) et si les vérifications associées à la transition demandée sont satisfaites (54).

18. Procédé selon l'une quelconque des revendications 15 à 17, caractérisé en ce qu'il comprend en outre une étape (55) d'exécution d'actions négatives consistant à exploiter une entrée (400, 403, 406), correspondant à la transition demandée, de la table (13) d'actions, dans le cas où les vérifications associées à la transition demandée ne sont pas satisfaites (54).

19. Procédé selon l'une quelconque des revendications 11 à 14, ledit procédé étant mis en oeuvre au sein de l'objet, à la suite d'une demande de transition d'un premier état additif vers un second état additif, caractérisé en ce qu'il comprend :

- une étape (511) de validation de l'autorisation de ladite demande consistant à analyser une extension (16) de la table (11) des transitions possibles;
- une étape (512) d'évaluation des vérifications associée à la transition demandée consistant à exploiter une entrée (33) d'une extension (17) de la table (12) des vérifications;

- une étape (517) de modification de l'état courant de l'objet si et seulement si la transition demandée est autorisée (511) et, si les vérifications de la configuration de l'objet sont satisfaites (514).

20. Procédé selon la revendication 19, caractérisé en ce qu'il comprend en outre une étape (513) d'exécution d'actions systématiques en analysant une entrée (407, 408, 411), correspondant à la transition demandée, d'une extension (18) d'une table (13) d'actions .

21. Procédé selon l'une quelconque des revendications 19 ou 20, caractérisé en ce qu'il comprend en outre une étape (516) d'exécution d'actions positives en analysant une entrée (407, 409, 412), correspondant à la transition demandée, d'une extension (18) d'une table (13) d'actions demandée si :

- la transition demandée est autorisée (511)
- et, si les vérifications associées à la transition demandée sont satisfaites (514).

22. Procédé selon l'une quelconque des revendications 19 à 21, caractérisé en ce qu'il comprend en outre une étape (515) d'exécution d'actions négatives en analysant une entrée (407, 410, 413), correspondant à la transition demandée, d'une extension (18) d'une table (13) d'actions dans le cas où les vérifications associées à la transition demandée ne sont pas satisfaites (514).

23. Procédé selon l'une quelconque des revendications 11 à 14, ledit procédé étant mis en oeuvre, au sein de l'objet, à la suite d'une demande de transition d'un état de référence vers un état additif, caractérisé en ce qu'il comprend :

- une étape (528) de validation de l'autorisation de d'une transition dudit état de référence vers un état additif en analysant la table (11) des transitions possibles;

- une étape (521) de validation de l'autorisation de d'une transition dudit état de référence vers ledit état additif en exploitant une extension (16) d'une table (11) des transitions possibles;

- une étape (522) d'évaluation des vérifications associée à la transition demandée en exploitant une entrée (33) d'une extension (17) d'une table (12) des vérifications;

- une étape (527) de modification de l'état courant de l'objet si et seulement si la transition demandée est autorisée (528, 521) et, si les vérifications de la configuration de l'objet sont satisfaites (524).

24. Procédé selon la revendication 23, caractérisé en ce qu'il comprend en outre une étape (523) d'exécution d'actions systématiques en exploitant une entrée (407, 408, 411), correspondant à la transition demandée, d'une extension (18) d'une table (13) d'actions.

25. Procédé selon l'une quelconque des revendications 23 ou 24, caractérisé en ce qu'il comprend en outre une étape (526) d'exécution d'actions positives en exploitant une entrée (407, 409, 412), correspondant à la transition demandée, d'une extension (18) d'une table (13) d'actions si:

- la transition demandée est autorisée (528, 521)

- et, si les vérifications associées à la transition demandée sont satisfaites (524).

26. Procédé selon l'une quelconque des revendications 23 à 25, caractérisé en ce qu'il comprend en outre une étape (525) d'exécution d'actions négatives en exploitant une entrée (407, 410, 413), correspondant à la transition demandée, d'une extension (18) d'une table (13) d'actions dans le cas où les vérifications associées à la transition demandée ne sont pas satisfaites (524).

27. Procédé selon l'une quelconque des revendications 11 à 26, caractérisé en ce que ledit procédé n'autorise pas le franchissement d'une transition d'état, d'un état additif vers un état de référence.

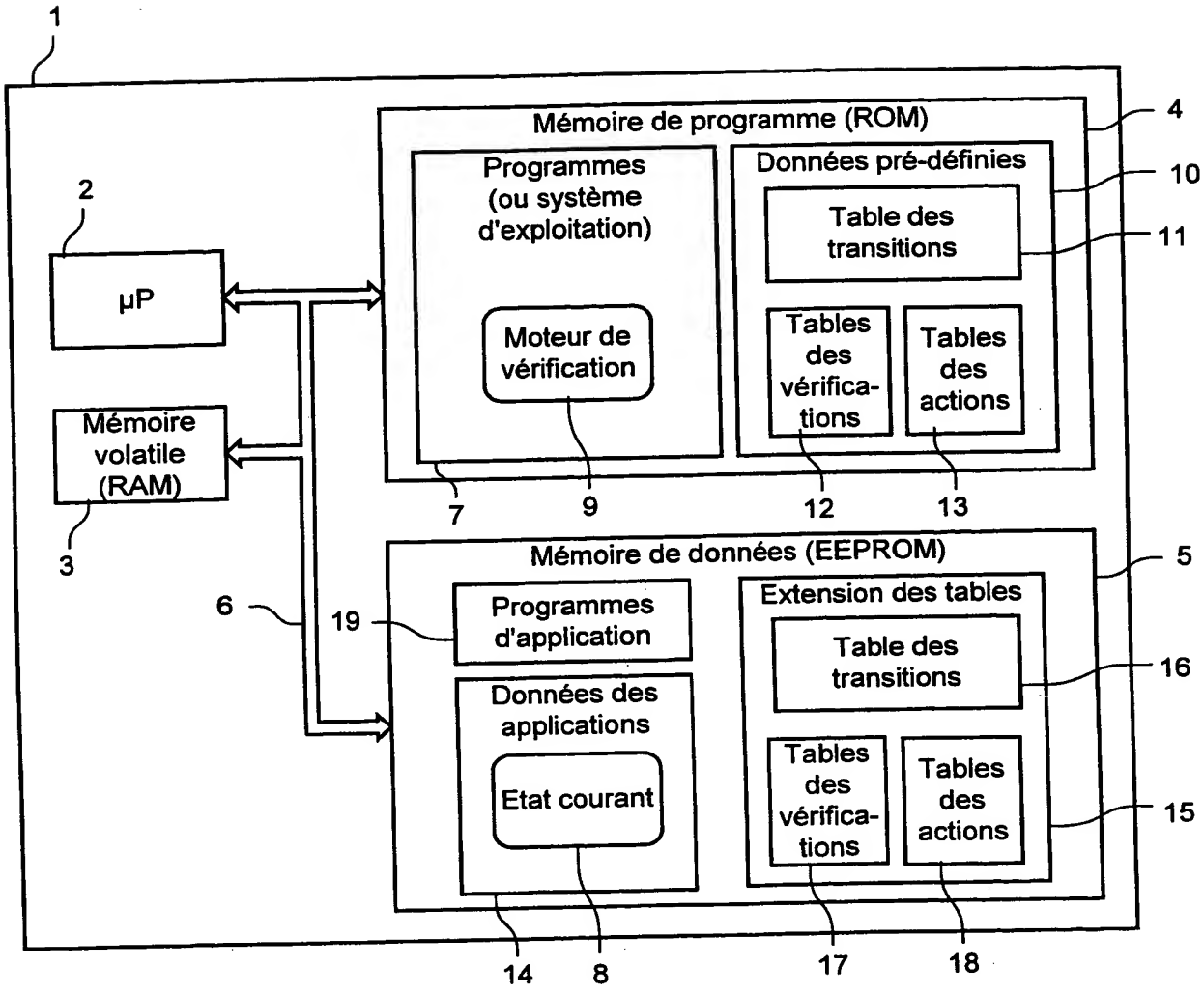
1
Mémoire de programme (ROM)
4
Programmes (ou système d'exploitation)
Données pré-définies
10
2
Table des transitions
11
µP
Moteur de vérification
Tables des vérifica-tions
Tables des actions
Mémoire volatile (RAM)
3
7
9
12
13
Mémoire de données (EEPROM)
5
6
19
Programmes d'application
Extension des tables
Table des transitions
16
Données des applications
Etat courant
Tables des vérifica-tions
Tables des actions
15
14
8
17
18

FIG. 1

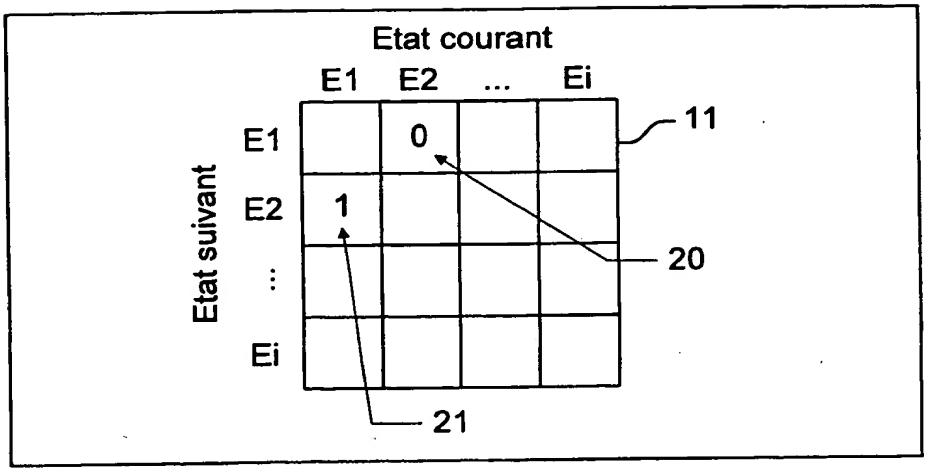
Etat courant
E1
E2
...
Ei
Etat suivant
E1
E2
Ei
0
1
11
20
21

FIG. 2a

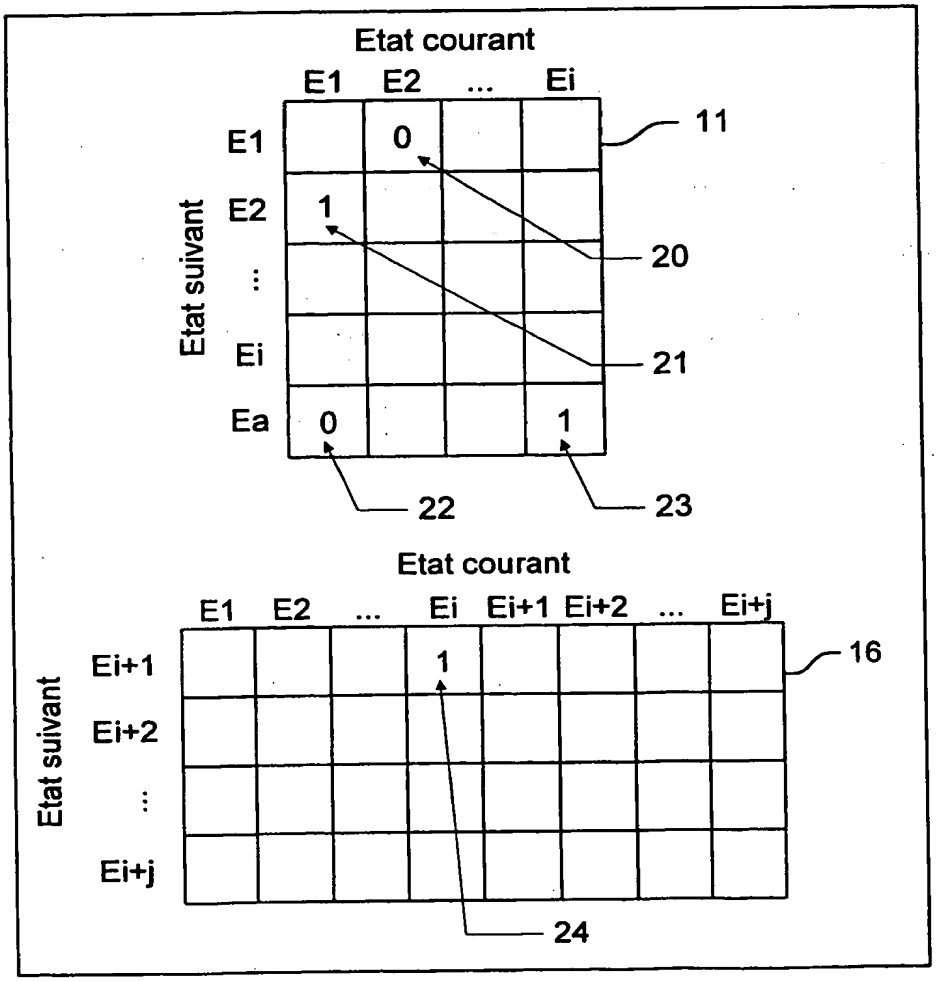
Etat courant
E1
E2
...
Ei
Etat suivant
E1
E2
Ei
Ea
0
1
11
20
21
22
23
Etat courant
E1
E2
...
Ei
Ei+1
Ei+2
Ei+j
Etat suivant
Ei+1
Ei+2
Ei+j
1
16
24

FIG. 2b

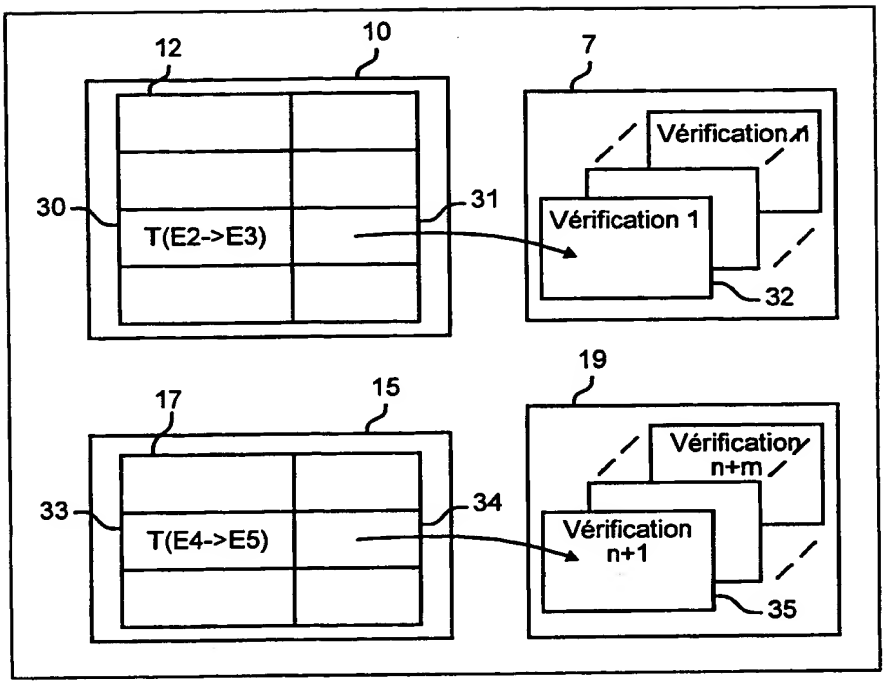
12
10
7
Vérification n
Vérification 1
30
T(E2->E3)
31
32
19
17
15
Vérification n+m
33
T(E4->E5)
34
Vérification n+1
35

FIG. 3

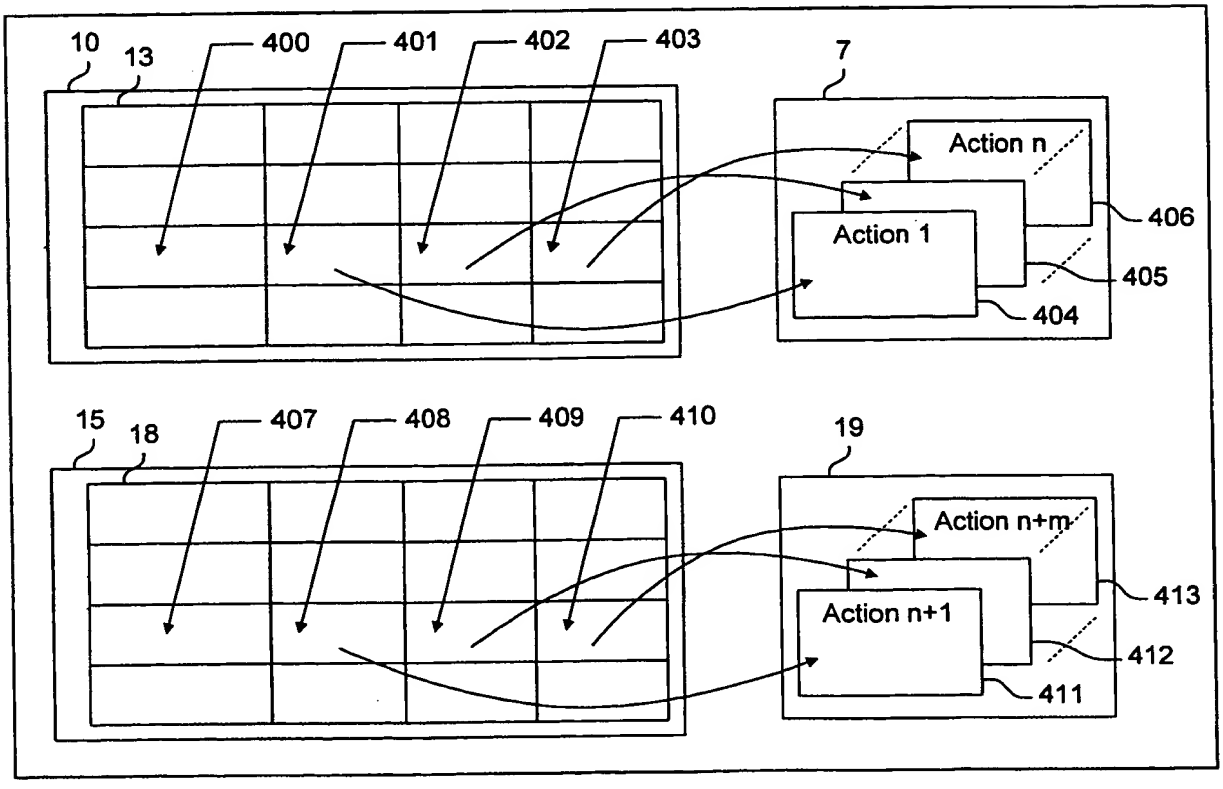
10
13
400
401
402
403
7
Action n
Action 1
406
405
404
15
18
407
408
409
410
19
Action n+m
Action n+1
413
412
411

FIG. 4

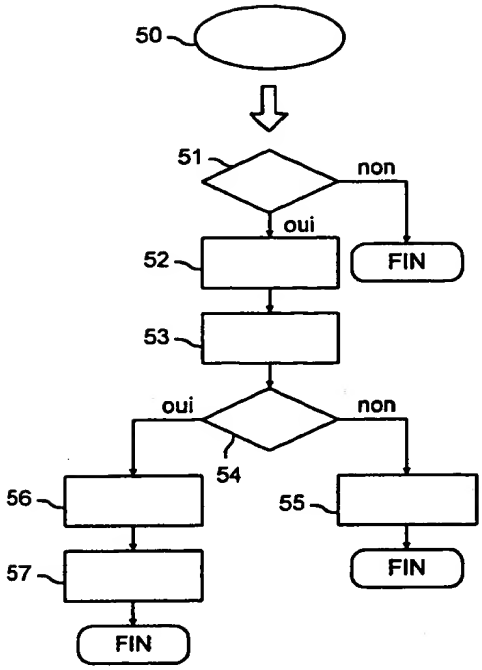


FIG. 5a

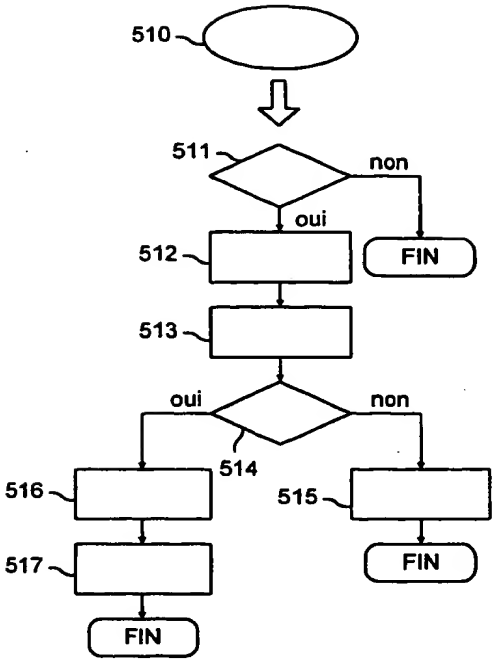


FIG. 5b

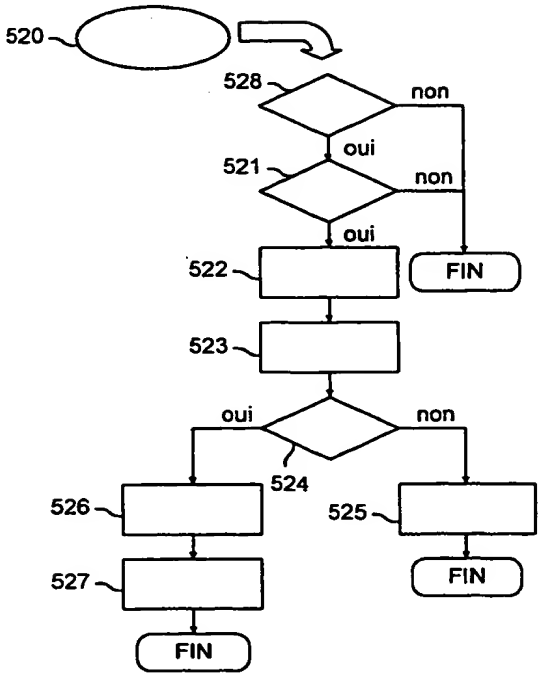


FIG. 5c

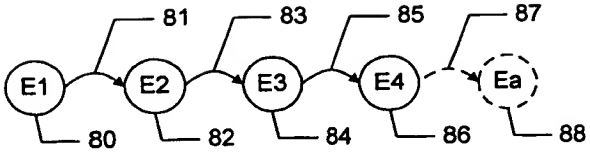


FIG. 6a

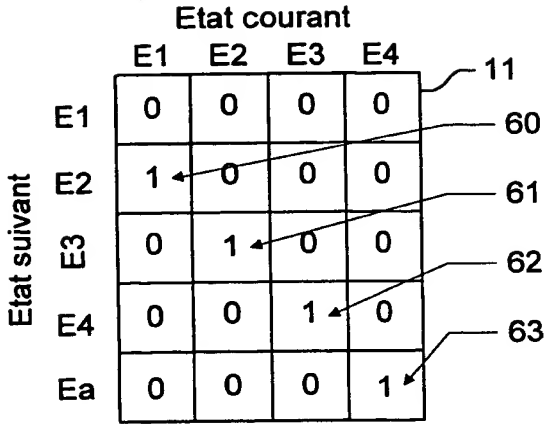


FIG. 6b

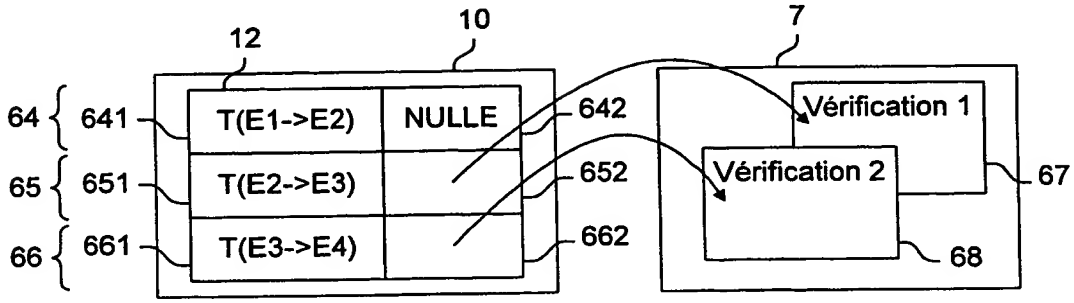


FIG. 6c

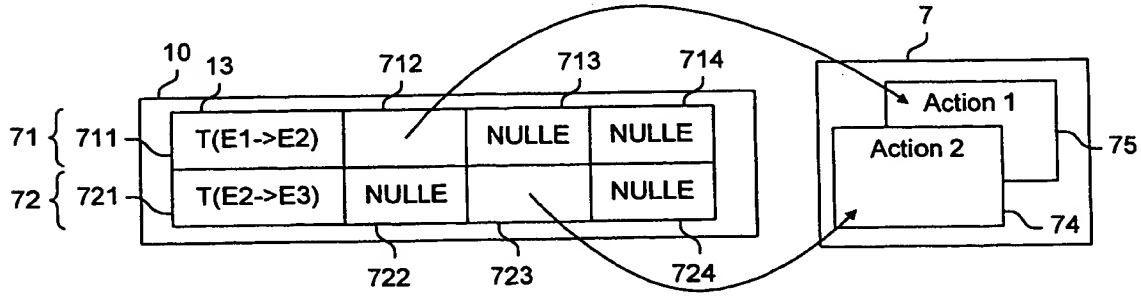


FIG. 6d